Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

CTIA
1400 16th Street NW, Suite 600
Washington, D.C. 20036
202-736-3200

November 15, 2021

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

COMMENTS OF CTIA

CTIA[1] welcomes the opportunity to submit these comments on the Federal Communications Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking in the above-referenced proceeding ("NPRM"), in which the Commission seeks comment on proposed updates to its Customer Proprietary Network Information ("CPNI") rules and Local Number Portability ("LNP") rules to further protect consumers from subscriber identity module ("SIM") swapping and port-out fraud.[2] CTIA and its members agree with the Commission that SIM swapping and port-out fraud are problems that require continued attention and look forward to collaborating to advance the shared goal of protecting consumers from fraud.[3]

I. INTRODUCTION AND SUMMARY

CTIA and its members agree with the Commission's goal to "put[] an end to" SIM swapping and port-out fraud, which put consumers, the telephone network, and other businesses

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Protecting Consumers from SIM Swap and Port-Out Fraud, Notice of Proposed Rulemaking, FCC 21-102, WC Docket No. 21-341, ¶¶ 1-3 (Sept. 30, 2021) ("NPRM").

[3] *Id.* ¶ 22.

at risk.[4] Wireless providers take SIM swapping and port-out fraud very seriously and have been working constantly to combat the sophisticated and evolving tactics of the bad actors behind these schemes with innovative tools and evolving countermeasures. Today, well over 99% of SIM swap and port-out requests are legitimate, but the wireless industry remains focused on combatting the fraudulent requests that do occur.

As the Commission takes steps to root out this fraud, it is critical to understand that wireless providers cannot be the only line of defense against SIM swapping and porting schemes. All actors across the mobile and Internet ecosystem—including financial and social media companies whose users' accounts are often targeted—must work together to thwart the bad actors that perpetrate these crimes. In particular, with respect to SIM swapping fraud, companies across the economy that authenticate their customers must decide how best to do so, based on well-founded principles of risk management. Mobile accounts may not always be an appropriate basis for third-party apps and services to authenticate their end users. To illustrate, a mobile device SIM card was originally intended to enable service flexibility, competition, and consumer choice—not for off-network identity authentication of a third-party's end users. Accordingly, third-party apps and services, such as cryptocurrency services, must make risk-based decisions before relying on SIM cards and the accounts associated with them to authenticate an end user. This is especially true for high-stakes financial transactions or other activity that consumers want to safeguard. Additionally, while wireless providers support robust anti-fraud policies, the Commission must balance such policies with other important goals, including continuity of reliable service, assurance of public safety, and promotion of competition and consumer choice, given the ever-growing importance of wireless services to consumers.

[4] *Id.* ¶ 2.

Accordingly, CTIA supports flexible and balanced efforts targeted at preventing SIM swapping and port-out fraud as one prong of a multi-prong, all-stakeholder offensive against fraudsters to protect consumers. CTIA generally supports the goals of the Commission's proposed rules in Appendix A of the NPRM, and with these comments, CTIA suggests adjustments to ensure that the FCC's approach is flexible and future-proof, so providers can continue to use cutting-edge tools to remain ahead of bad actors, while addressing the unique needs of their customers and networks and managing operational hurdles. Regarding the additional policy approaches raised throughout the NPRM beyond what is proposed in Appendix A, CTIA encourages the Commission to form a multi-stakeholder working group so that experts across sectors can study these complex issues to ensure that the Commission's anti-fraud efforts involve all stakeholders and do not have unintended consequences for consumers.

II. ALL STAKEHOLDERS MUST BE ENGAGED TO PROTECT CONSUMERS FROM SIM SWAPPING AND PORT-OUT FRAUD.

A. The Wireless Industry Takes Consumer Fraud Seriously and Works to Stay Ahead of Bad Actors with Innovative Security Approaches.

The wireless industry and the Commission share the goal of protecting consumers from fraud—full stop. Indeed, it is in the wireless industry's best interest to promote device and account security and to prevent fraudulent SIM swapping and porting, as doing so protects customers and maintains trust in the network. To this end, the wireless industry has committed immense resources to combat these types of fraud, taking a multi-pronged approach to protecting subscribers, which combines internal system protections with consumer-facing safeguards.

To stay ahead of the persistent fraudsters and evolving tactics, the wireless industry constantly deploys new tools and improvements to thwart fraud. While each provider's practices are different and many are not publicly visible so as to shield provider tactics from criminals, examples of the variety of tactics used to combat SIM swapping and port-out fraud include:

- Offering wireless account as well as SIM card PINs or passcodes and/or the ability to lock or freeze wireless accounts to protect against unauthorized access and changes
- Employing multi-factor authentication when account changes are requested, including one-time passcodes sent via text message, among other techniques
- Providing additional consumer-facing security tools to further protect accounts, as well as online instructional videos on how to use such tools
- Training employees to identify signs of a fraudulent SIM swap request and uses
- Leveraging technology to identify and combat unauthorized SIM swaps
- Working with financial institutions on ways to prevent fraud via SIM swap activity
- Working with law enforcement to bring action against SIM swap fraudsters
- Notifying customers when a SIM swap is initiated

Providers collaborate to address attempted fraud and explore authentication options at an industry-level as well. For example, CTIA members participate in the Number Portability Industry Forum, which created voluntary best practices that address unauthorized and fraudulent ports.[5] As another example, major national wireless providers joined forces to develop an authentication tool—ZenKey.[6]

Additionally, the wireless industry comes together to educate consumers. CTIA provides resources for consumers on steps that they can take to protect their wireless accounts, including establishing a PIN that is required for account access, using a number that cannot be easily determined; downloading the provider's mobile app to stay up to date on security updates and alerts; and following providers' security advisories and leveraging tools such as multi-factor authentication.[7]

[5] *See* NPRM ¶ 21.
[6] *See About Us*, ZenKey, https://myzenkey.com/aboutus/ (last visited Nov. 10, 2021).
[7] *See Protecting Your Wireless Account Against SIM Swap Fraud*, CTIA Consumer Resources, https://www.ctia.org/protecting-against-sim-swap-fraud (last visited Nov. 10, 2021).

B. Addressing SIM Swapping and Port-Out Fraud Head On Will Require Risk-Informed Work by All Stakeholders Across the Mobile and Internet Ecosystem.

All stakeholders in the mobile and Internet ecosystem must play their part to protect consumers. Wireless providers cannot be the only line of defense against criminal fraudsters and scammers behind SIM swapping and port-out fraud, which are often part of broader schemes to do harm to consumers.

Financial and Social Media Service Providers. A fight against this type of fraud cannot be waged without the participation of the providers of financial and social media services whose customer accounts the fraudsters most often seek to access. Scammers perpetrating unauthorized SIM swaps often target financial accounts and social media accounts for the purpose of gaining unauthorized access, and as such, it is imperative for financial institutions, cryptocurrency services, social media platforms, and others whose users' accounts are being targeted to adopt aggressive and risk-informed measures to help protect consumers.

One tool to bolster security and protect consumers in certain scenarios is multi-factor authentication. Financial institutions, social media platforms, and others authenticating their users through this tool must take a prudent approach and understand there is no one-size-fits-all tool for authentication. No method addresses all security concerns and no authentication factors will ever be without risk. Even physical tokens can be stolen. SMS text messaging may be an appropriate authentication factor, depending on the nature and the sensitivity of the information being accessed and whether the consumer maintains control over the device and the number associated with it. SMS-based two-factor authentication, however, should not be the only tool to defend against account takeovers. While SMS-based two-factor authentication may be perfectly suitable to some settings, it may not uniformly be appropriate for all types of transactions. As the FTC recently recognized in updating its Safeguards Rules:

> [i]n some cases, use of SMS text messages as a factor may be the best solution because of its low cost and easy use, if its risks do not outweigh those benefits under the circumstances. In other instances, however, the use of SMS text messages may not be a reasonable solution, such as when extremely sensitive information can be obtained through the access method being controlled, or when a more secure method can be used for a comparable price. A financial institution will need to evaluate the balance of risks for its situation.[8]

Accordingly, if the financial stakes are high, consumers and entities like financial institutions that are authenticating end users may need to augment their security approaches. Logging into a social media account may require one level of authentication, whereas a $10,000 transaction may require heightened measures, and ultimately it is up to the organization authenticating end users to make that risk-based decision. Importantly, in addition to SMS-based authentication, these companies also have other robust authentication tools at their disposal. For example, there are biometrics features that exist on devices, and even beyond device-level tools, innovation abounds in the authentication space, including from third-party providers. These types of options can add layers of protection to sensitive transactions and data, as appropriate based on the risk.

In sum, the critical role of financial institutions, cryptocurrency services, and social media platforms in the fight against SIM swapping and port-out-fraud cannot be overstated. While the FCC and wireless providers can work aggressively to root out fraud, we must also work together with these other entities to protect consumers. Already, the wireless industry has developed tools and processes to coordinate across the ecosystem to prevent fraud.[9] Looking ahead in the fight to protect consumers from the bad actors behind fraudulent SIM swapping and

---

[8] FTC Standards for Safeguarding Customer Information, Final Rule, 16 C.F.R. § 314, at 23-24 (Oct. 27, 2021), https://www.ftc.gov/system/files/documents/federal_register_notices/2021/10/safeguards_rule_final.pdf.

[9] One example is Neustar's Phone Takeover Risk product for enterprises. *See Phone Takeover Risk*, Neustar, https://www.cdn.neustar/resources/product-literature/risk/neustar-phone-diversion-solution-sheet.pdf (last visited Nov. 10, 2021).

porting, this type of collaboration will be key. CTIA encourages the FCC, as the expert agency when it comes to telecommunications, to similarly work together with appropriate stakeholders from other sectors—including but not limited to the financial sector—to lead a coordinated and comprehensive approach to stopping SIM swapping and port-out fraud. As discussed below, a multi-stakeholder working group to explore best practices is one way the FCC can engage in this important, cross-sector work.[10]

Law Enforcement. Enforcement entities also play an important role in preventing the proliferation of this type of fraud. Targeting and stopping the bad actors that perpetrate SIM swapping and port-out fraud should be a priority across federal and state enforcement agencies with appropriate authority. Wireless providers already diligently refer instances of fraud to law enforcement and otherwise work closely with law enforcement on these matters, as needed.

Consumer Education. All stakeholders must also work to educate consumers about protecting personal data and accounts. As highlighted above, the wireless industry prioritizes consumer education and provides resources to explain these schemes and empower consumers to take steps to protect themselves, alongside other work the industry does to prevent consumer fraud. Law enforcement can also educate consumers about the evolving threats and steps they can take to protect themselves.[11] Additionally, the FCC provides resources for consumers, including a consumer guide on cell phone fraud.[12] Consumer education is a critical element in combatting fraud and should continue to be a focus.

---

[10] *See, infra* Section V(B).

[11] *See, e.g., FBI San Francisco Warns the Public of the Dangers of SIM Swapping, Criminals Are Targeting Victims with Cryptocurrency and Other Digital Currency Accounts,* FBI San Francisco (March 6, 2019), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping.

[12] *See Cell Phone Fraud,* FCC Consumer Guides, https://www.fcc.gov/consumers/guides/cell-

III. THE COMMISSION'S WORK TO COMBAT FRAUD MUST PRESERVE IMPORTANT SERVICE RELIABILITY, PUBLIC SAFETY, AND COMPETITION GOALS.

A. The Commission and Wireless Providers Must Balance the Goals of Providing Critical Wireless Services While Preventing Fraud.

Providing reliable and flexible wireless service to customers is of paramount importance and wireless operators embrace this responsibility. As the Commission rightly emphasizes in the NPRM, "cell phones are an essential part of everyday life for most Americans."[13] Indeed, it is difficult to overstate the ever-growing importance of wireless service for consumers. In 2020, CTIA estimates 468.9 million total wireless connections in the U.S., a number that has steadily grown year-over-year.[14] Accordingly, any Commission effort to address SIM swapping and port-out fraud must balance the dual goals of (1) providing seamless and accessible services and not unduly burdening legitimate SIM swaps and port-out requests that ensure that consumers have access and choice in wireless services, and (2) stopping fraud.

CTIA and its members agree with the Commission that instances of fraud must be stopped and are ready to work with the agency to "put[] an end to [these] two methods used by bad actors to take control of consumers cell phone accounts and wreak havoc on people's financial and digital lives," while at the same time ensuring that provision of service to consumers is not degraded and that legitimate requests can be addressed.[15] In developing policy approaches to help providers achieve both goals, it is critical for the Commission to understand that well over 99% of SIM swap and port-out requests are legitimate.

---

phone-fraud (last visited Nov. 10, 2021).

[13] NPRM ¶ 1.

[14] *2021 Annual Survey Highlights*, CTIA, at 10 (July 27, 2021), https://www.ctia.org/news/2021-annual-survey-highlights.

[15] NPRM ¶ 2.

While the Commission asks several questions about impacts to legitimate consumer requests and public safety,[16] certain discussions in the NPRM raise questions about the careful balance of service provision and fraud prevention. For example, mandating a strict 24-hour delay in the case of a SIM swap request,[17] or where there are multiple failed authentication requests related to a SIM swap request,[18] would be extremely onerous for consumers and would adversely impact the critical need for timely and legitimate SIM swaps. This type of blanket requirement would also make it exceedingly difficult for a consumer to obtain a new phone and continued service when a device breaks or is lost, representing a full day where that consumer could not rely on their wireless service for a range of activities, from "keep[ing] in touch with friends through voice calls [and] text messages" to placing life-saving public safety calls.[19] Service disruptions due to strict authentication requirements could be particularly impactful for customers who are in emergency situations. To better balance these important goals, rather than mandating waiting periods, the Commission should clarify that providers have flexibility to implement such delays as appropriate to address the unique circumstances of any given request or consumer. For example, a short delay—where a consumer would be able to respond to a push notification, text message, or other notification to speed up the process—may be appropriate in some situations and could help to prevent fraud while balancing important service goals.

[16] *See, e.g., id.* ¶ 33 ("We seek comment on what processes carriers can implement to prevent bad actors from attempting multiple authentication methods while at the same time ensuring that protections do not negatively impact legitimate customer requests."); *id.* ¶ 37 ("How burdensome would such a [24-hour] delay be for customers? Are there safety implications for customers who legitimately need a new SIM? Could such a delay prevent the customer from completing 911 calls during the waiting period?").
[17] *Id.* ¶ 37.
[18] *Id.* ¶ 33.
[19] *Id.* ¶ 1.

B. The Commission Should Be Careful That Any Anti-Fraud Rules Do Not Undermine Consumers' Ability to Receive Wireless Services from the Provider of Their Choice.

Beyond provision of service, competition and consumer choice are goals that the Commission and providers must prioritize, in addition to fraud prevention. The Commission should weigh potential impacts on these critical goals when crafting an approach to combat SIM swapping and port-out fraud. This is especially true in the context of the LNP rules, where the Commission recognizes it must be mindful of "competing goals of protecting customer information and promoting competition through local number porting."[20]

It is critical that the LNP rules continue to protect against anti-competitive behaviors, and that any updates to address port-out fraud should be clearly tied to consumer fraud protection. The Commission should be wary of imposing rules that could be manipulated to inhibit consumers' ability to use the mobile carrier of their choice while also retaining their assigned telephone number.

IV. FLEXIBILITY IS KEY TO FUTURE-PROOF THE FCC'S GUIDANCE AND TO ENABLE PROVIDERS TO STAY ON THE CUTTING-EDGE OF FRAUD RISK MANAGEMENT.

A. A Flexible Anti-Fraud Approach Will Enable Providers to Deploy Innovative Authentication Tools to Stay Ahead of Fraudsters.

Any Commission approach to preventing fraud should allow providers to innovate and deploy a diverse range of tools to stay ahead of bad actors and evolve strategies as fraudulent tactics rapidly change. Flexibility is a cornerstone of effective risk management, as it allows providers to develop and deploy innovative tools that can meet evolving threats and stay ahead of the fraudsters, as opposed to "checking the box" on stagnant compliance requirements. The National Institute of Standards and Technology ("NIST") describes that its seminal

[20] *Id.* ¶ 53.

Cybersecurity Framework "encourages technological innovation by aiming for strong cybersecurity protection without being tied to specific offerings or current technology," explaining that flexibility allows organizations to "make choices among products and services available in the marketplace."[21]

Alternatively, rigid and prescriptive requirements hurt security more than they may help. To this point, the NPRM asks whether "requiring specific methods of authentication provides a 'roadmap' to bad actors."[22] The answer is a resounding yes. Fraudsters and scammers are savvy; if every provider authenticates requests in the same way, fraudsters and scammers will find a way around such uniform "safeguards." This will lead to a constant cycle of regulation trying to keep up with the bad actors—with consumers coming in last. Further, avoiding rigid rules that are tied to specific technologies or tools will also help to future-proof FCC guidance when it comes to authentication. Authentication best practices from 2007 are different than they are today, and they will surely be different in another ten to fifteen years. The Commission should build in flexibility to allow for its framework to evolve with time and technology.

In the NPRM, the standard proposed in Appendix A to authenticate SIM changes rightly starts from the principle of flexibility. With that said, the Commission should take even more steps to ensure that the proposed rule will best protect consumers by allowing providers to adjust their authentication approaches to the ever-changing tactics from bad actors, all the while not providing those bad actors with a roadmap to circumvent the providers' efforts. Specifically, the proposed rule would establish a general standard for providers to securely authenticate customers

[21] *See Questions and Answers*, NIST Cybersecurity Framework, *https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics* (last visited Nov. 10, 2021).
[22] NPRM ¶ 27.

before effectuating a SIM change. It lists several authentication methods as secure examples and explicitly states that "[t]hese methods shall not be considered exhaustive and an alternative customer authentication measure used by a carrier must be a secure method of authentication."[23] While CTIA suggests several adjustments to this standard, as detailed below,[24] CTIA fully supports the principle of flexibility that drives the proposal.

Notwithstanding the proposal in Appendix A, the NPRM asks questions that appear to favor a more prescriptive approach. For example:

- The NPRM asks, "[i]f [the Commission adopts] a specific set of authentication practices that carriers must employ before effectuating a SIM change, how can [it] account for changes in technology, recognizing that some of these methods may become hackable over time, while additional secure methods of authentication will likely be developed over time?"[25]
- With respect to the number porting rules, the Commission asks whether it should "require all carriers to implement any of the additional authentication processes for wireless port requests some providers have already developed and implemented."[26]
- The Commission asks whether mandating the same authentication requirements on all wireless port-out requests would "reduce consumer confusion."[27]
- The NPRM also asks whether the Commission should "require carriers to comply with the NIST Digital Identity Guidelines, which are updated in response to changes in technology, in lieu of other proposals."[28]

The Commission has recognized the value of flexibility in the past,[29] and indeed it did so with the proposed rule in Appendix A. It should not stray from this sound approach by mandating

[23] *See* NPRM, Appendix A (proposed 47 C.F.R. § 64.2010(e)).
[24] *See infra* Section V(A).
[25] NPRM ¶ 27.
[26] *Id.* ¶ 55.
[27] *Id.*
[28] *Id.* ¶ 28.
[29] *See, e.g., Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd. 4876, ¶ 34 (2019) (explaining—in the context of offering call blocking programs based on reasonable analytics—that "limiting opt-out call-blocking programs to rigid blocking rules that prescribe in detail when a voice service provider may block is unnecessary when consumers have the option to opt out, could enable callers to evade blocking,

rigid and prescriptive rules that will hinder multi-pronged efforts to keep consumers' information secure. Specifically with respect to the Commission's questions about NIST's Digital Identity Guidelines, CTIA cautions that while providers can draw from NIST's work, they should not be bound by authentication guidance tailored for federal agency use.[30]

Similarly, the Commission should refrain from adopting a singular focus on specific vulnerabilities or threats, as these dynamics will undoubtedly shift over time. The NPRM discusses specific vulnerabilities[31] and relies on the Princeton Study,[32] which looks at one snapshot in time, within a single context, of an evolving set of threats and practices. While the Commission should certainly keep apprised of specific threats, the agency must be mindful not to craft an approach that is too narrowly focused on the threats of today. Indeed, the Commission's past findings in the 2007 CPNI Order bear this out, explaining that "techniques for fraud vary and tend to become more sophisticated over time" and carriers "need leeway to engage emerging threats."[33] This is even truer today than it was in 2007. As cybercriminals become more sophisticated and move beyond SIM card swaps and port-out fraud, the industry

---

and could impede the ability of voice service providers to develop dynamic blocking schemes that evolve with calling patterns").

[30] *See* NIST Special Publication 800-63-3, Digital Identity Guidelines, NIST, at iii (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf ("These guidelines provide technical requirements *for federal agencies* implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose." (emphasis added)); *see also* NPRM ¶ 28 ("The NIST Digital Identity Guidelines are a set of guidelines that provide technical requirements *for federal agencies* 'implementing digital identity services'" (emphasis added)).

[31] *See* NPRM ¶ 24.

[32] *See id.* ¶ 9.

[33] *See id.* ¶ 27 (quoting *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927, ¶ 33 (2007)).

will need the flexibility to innovate and build effective barriers against eventual new forms of customer account attacks.

B. Providers Need Flexibility to Address the Needs of Customers, Meet Operational Challenges, and Avoid Unintended Consequences.

There is no one-size-fits-all solution to prevent consumer fraud. Providers face different threats and challenges with respect to different services, offerings, and customers, even within the same organization. These varied circumstances require varied approaches.

One example of this arises in the context of pre-paid versus post-paid services. Fighting fraud in the pre-paid context is different than in the post-paid context, but the goal is the same: that all consumers' mobile identities are protected while they have access to service.[34] As compared to post-paid plans, providers ordinarily do not collect or have detailed identity information for pre-paid customers.[35] This lack of information makes it more difficult to rely on a user's mobile phone number for authentication purposes. However, it should not impede a diverse range of consumers from accessing wireless connectivity.

As such, the Commission is right to inquire about the differences between pre-paid and post-paid accounts. It should ensure that with its anti-fraud actions, wireless providers have the flexibility to safeguard against fraud while maintaining a robust pre-paid market, which serves approximately 74.1 million pre-paid subscribers across the nation[36] and promotes consumer

---

[34] *See id.* ¶ 73 ("Invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.").

[35] As the Commission has explained, "prepaid subscribers may lack the credit background or income necessary to qualify for postpaid service. To prevent credit losses and mitigate the credit risk associated with the prepaid segment, service providers require advance payment for both prepaid service and handsets." *Communications Marketplace Report,* GN Docket No. 20-60, 2020 Communications Marketplace Report, 36 FCC Rcd. 2945, n.119 (2020).

[36] Jake Lestock, CTIA, Testimony before the Massachusetts Joint Comm. On Pub. Safety and Homeland Sec. (July 14, 2021), https://api.ctia.org/wp-content/uploads/2021/07/CTIA-

choice, flexibility, and access to quality services and devices that satisfy diverse consumer needs.[37]

The Commission should recognize that the goals of authentication and service flexibility can be at odds—especially in the pre-paid context. Specifically, the NPRM's more onerous and rigid authentication proposals would likely impact pre-paid customers differently than post-paid subscribers, especially where pre-paid customers may be at a higher risk of negative impacts due to a service disruption as a result of limited access to other forms of digital connectivity or access. One example is the proposed account freeze requirement that holds that where a consumer chooses to lock their account to prohibit unauthorized port requests, a "wireless provider shall not fulfill a simple wireless-to-wireless port order request until the customer deactivates the lock on the account."[38] This may negatively impact pre-paid customers whose devices are lost or stolen, as the pre-paid market offers consumers the option to purchase service with less identifiable information than post-paid, and thus information that may be necessary to deactivate a freeze may not have been provided when an account is initialized. Thus this may limit a consumer's ability to remove a freeze and validate an account where the consumer does not have a working device. Rather than rigid mandates that do not apply equitably or evenly across the different types of services, the Commission should establish flexible approaches that allow providers to protect consumers in both pre-paid and post-paid contexts.

Additionally, there may be unique operational hurdles that each provider faces in implementing certain safeguards and processes, and providers need flexibility to manage these

---

Testimony-in-Support-of-Massachusetts-H.2422-Prepaid-POS-.pdf.

[37] *See, e.g.*, Diana Goovaerts, *CTIA Hot Seat: AT&T's Glen Lurie Talks Video, 5G, IoT*, 5G Technology World (Sept. 7, 2016), https://www.5gtechnologyworld.com/ctia-hot-seat-atts-glenn-lurie-talks-video-5g-iot/.

[38] NPRM at Appendix A (proposed 47 C.F.R. § 52.37(e)).

obstacles. For example, developing procedures to track multiple failed authentication attempts as contemplated in the NPRM would be challenging for providers, as authentication attempts may occur across different settings (*e.g.*, in person, online, or over the phone) and they may occur at disparate times.[39] The related strict lock-out requirements (*e.g.*, a 24-hour freeze) discussed in the NPRM would also be exceedingly burdensome for customers.[40] Customers routinely forget their passcodes and may guess a few times before getting it right. Consumers who fail authentication for legitimate reasons should not be subject to strict lock-out requirements.

V. CTIA SUPPORTS TARGETED PROPOSALS THAT BUILD ON PROVIDERS' ALREADY ROBUST EFFORTS TO ROOT OUT FRAUD.

A. The Commission's Proposed Rules Should Be Adjusted to Maximize Flexibility, Which Will Best Protect Consumers and Prevent Fraud.

CTIA supports flexible and balanced efforts targeted at preventing SIM swapping and port-out fraud and generally supports the goals of the Commission's proposed rules in Appendix A. The changes suggested below will help to ensure that the Commission and providers can most effectively contribute to the cross-industry defense that must be waged against fraudsters, while still ensuring service reliability and promoting competition. These suggestions start from the premise that technical, rigid, and narrow requirements will not move the needle for consumer protection in the same way that a smart, flexible, future-proof, and risk-based framework will.

1. *Proposed CPNI Rules*

Authentication. As discussed above, the authentication requirements proposed in Appendix A start from the principle of flexibility: the Commission is right to propose a general standard for providers to use a secure method of authenticating its customers, without prescribing

[39] *Id.* at Appendix A (proposed 47 C.F.R. § 64.2010(f)).
[40] *See id.* ¶ 33.

the exact methods it must use.[41] Similarly, the Commission is right to state that the authentication methods it lists as secure "shall not be considered exhaustive and an alternative customer authentication measure used by a carrier must be a secure method of authentication."[42] The Commission should make additional adjustments in the same spirit, which will give carriers the flexibility to continue to deploy cutting edge techniques to identify bad actors and confirm that their customers with legitimate requests are who they say they are.

- *First*, the Commission should clarify that its standard for "secure" authentication is tethered to reasonableness. The standard should be amended as follows: "Telecommunications carriers shall not effectuate a SIM change unless the carrier uses a ***reasonably*** secure method of authenticating its customer."[43] Further, this concept of reasonableness should be carried through any time the rule mentions the "secure methods" standard. This change will reiterate that the standard is moored to core risk management tenets and will allow for new authentication techniques to address new challenges, based on the context facing carriers and customers.

- *Second*, the Commission should clarify that the methods it identifies as reasonably "secure" constitute safe harbors.[44] This will provide carriers with clear but flexible guidance, while avoiding the pitfalls of providing a roadmap to bad actors or encouraging a compliance mindset as opposed to a proactive one.

- *Third*, the Commission should expand its list of reasonably secure methods.[45] This list should represent the broad and diverse authentication ecosystem that exists today and will continue to expand into the future. In contrast, the Commission's current list—which narrowly highlights only passwords and passcodes—does not include other authentication options, including authentication via government-issued ID, authentication based on analytics or other tools, app-based authentication tools, or biometric authentication, among many growing options. The Commission should identify these categories of authentication options instead of focusing on specific techniques under one narrow category.

---

[41] *Id.* at Appendix A (proposed 47 C.F.R. § 64.2010(e)).
[42] *Id.*
[43] *Id.* (suggested edit added).
[44] *Id.*
[45] *Id.*

Beyond the proposed new rule to address authentication with respect to SIM swap requests, the Commission should take this opportunity to update its other authentication requirements under the CPNI rules, which do not reflect the most up-to-date authentication best practices. The same flexible and future-proof standard should apply to access to CPNI and authentication across all settings, not just for SIM swaps.

Procedures for Failed Authentication Requests. Also as discussed above, there are significant challenges for providers associated with tracking and imposing requirements based on failed authentication requests. To give providers the flexibility needed to address challenges without imposing burdens on consumers or sacrificing other goals, the proposed requirement for carriers to develop, maintain, and implement procedures for responding to multiple failed authentication attempts should also be tethered to a reasonableness standard, as follows: "Wireless carriers shall develop, maintain, and implement procedures for responding to multiple failed authentication attempts***, where a carrier has reason to believe such attempts are fraudulent***."[46]

Notification of Account Changes. The rule as proposed in Appendix A to require immediate customer notification in the event of any SIM swap request should be adjusted to account for the complexities of notifications in various contexts.[47] For example, where a phone is lost or stolen, certain notifications will not reach consumers. Additionally, notifications must be weighed against other goals, and in general, avoid unnecessary friction in the user experience or other unintended consequences, such as notice fatigue. With that said, there are many instances where notifications to consumers are appropriate and providers can and do make

[46] *Id.* at Appendix A (proposed 47 C.F.R. § 64.2010(f)) (suggested edit added).
[47] *Id.* at Appendix A (proposed 47 C.F.R. § 64.2010(h)).

reasonable efforts to provide them. The Commission's approach should account for these nuances and allow for some flexibility in its application that will best serve consumers and prevent fraud.

2. *Number Porting Rules Updates*

Passcode Field. While framed as an "optional standard data field," the language proposed with respect to passcode fields could be read to be overly restrictive.[48] The Commission should clarify that its language does not require the use of a passcode or foreclose the option for providers to use a porting-specific, one-time PIN. Both methods of authentication may be appropriate in different contexts.

Notification required after port request. Similar to notifications of account changes with respect to SIM swap requests, the notification standard proposed under the LNP rules should be flexible and future-proof, not tied to specific technologies.[49] The standard should also account for the complexities of consumer notification in the context of number porting. CTIA and wireless providers recognize the important role notifications can play when there is suspected fraud, which is why providers already deploy such notifications as appropriate.

Account freezes. As mentioned above, the prohibition on wireless providers being able to fulfill a simple wireless-to-wireless port order request without a customer first deactivating their account lock where that customer has chosen an account lock may have unintended and harsh consequences on pre-paid customers in the event they experience a lost or stolen phone.[50] The Commission should adjust its proposed rule regarding account freezes to prevent against this

[48] *Id.* at Appendix A (proposed 47 C.F.R. § 52.37(c)).
[49] *Id.* at Appendix A (proposed 47 C.F.R. § 52.37(d)).
[50] *Id.* at Appendix A (proposed 47 C.F.R. § 52.37 (e)).

uneven impact from a mandate, and instead allow wireless providers more flexibility to facilitate consumer choice and competition for all consumers.

B. The NPRM's More Broad-Ranging Proposals and Questions—Beyond the Proposals in Appendix A—Require Additional Stakeholder Input.

The NPRM reflects the complex nature of SIM swapping and port-out fraud measures, with in-depth and broad-ranging questions. The wireless industry welcomes this dialogue with the FCC and stands ready to work together to develop smart and targeted ways to protect consumers from fraud while continuing to provide a diverse range of reliable and competitive wireless services. As the Commission develops the record in this proceeding, it is critical to understand the full picture of this complex issue and not rely too heavily on a single, limited view. For example, the Princeton Study only provides a limited window into a complex problem. Any new FCC approach to these issues beyond what is proposed in Appendix A requires more study and more stakeholders for a more holistic and nuanced understanding of SIM swapping and port-out fraud.

Accordingly, CTIA recommends that the Commission convene a working group to study some of the broader questions raised in the NPRM. The working group should be comprised of experts from all relevant stakeholder groups, and it should be tasked with developing best practices for the entire ecosystem. Similar to the Hospital Robocall Protection Group that developed best practices for different stakeholders in the illegal robocall context (*i.e.*, voice service providers, hospitals, and the government),[51] a SIM swap and port fraud working group could study and develop best practices for wireless providers, providers of services whose users' accounts are targeted, and enforcers who can pursue bad actors.

[51] *See Hospital Robocall Protection Group*, FCC, https://www.fcc.gov/hospital-robocall-protection-group.

As many of the issues raised in the NPRM are complex and require collaborative, stakeholder engagement to address, the Commission must develop a full record and ideally establish a working group prior to proposing any new regulatory approaches beyond what is in Appendix A. At a minimum, the Commission should commit to issuing a Further Notice of Proposed Rulemaking before moving forward with policies related to the broad questions asked in the NPRM that are not accompanied by proposed rule changes.

VI. CONCLUSION

CTIA welcomes the opportunity to work with the Commission to build from providers' already robust anti-fraud efforts and continue to protect consumers from SIM swapping and port-out schemes. While a flexible and balanced approach for wireless providers can be one aspect of this multi-pronged approach, wireless providers cannot be the only line of defense. An all-stakeholder offensive against the criminals behind these crimes will best protect consumers.

Respectfully submitted,

/s/ Melanie K. Tiano
Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street NW, Suite 600
Washington, D.C. 20036
202-736-3200

November 15, 2021